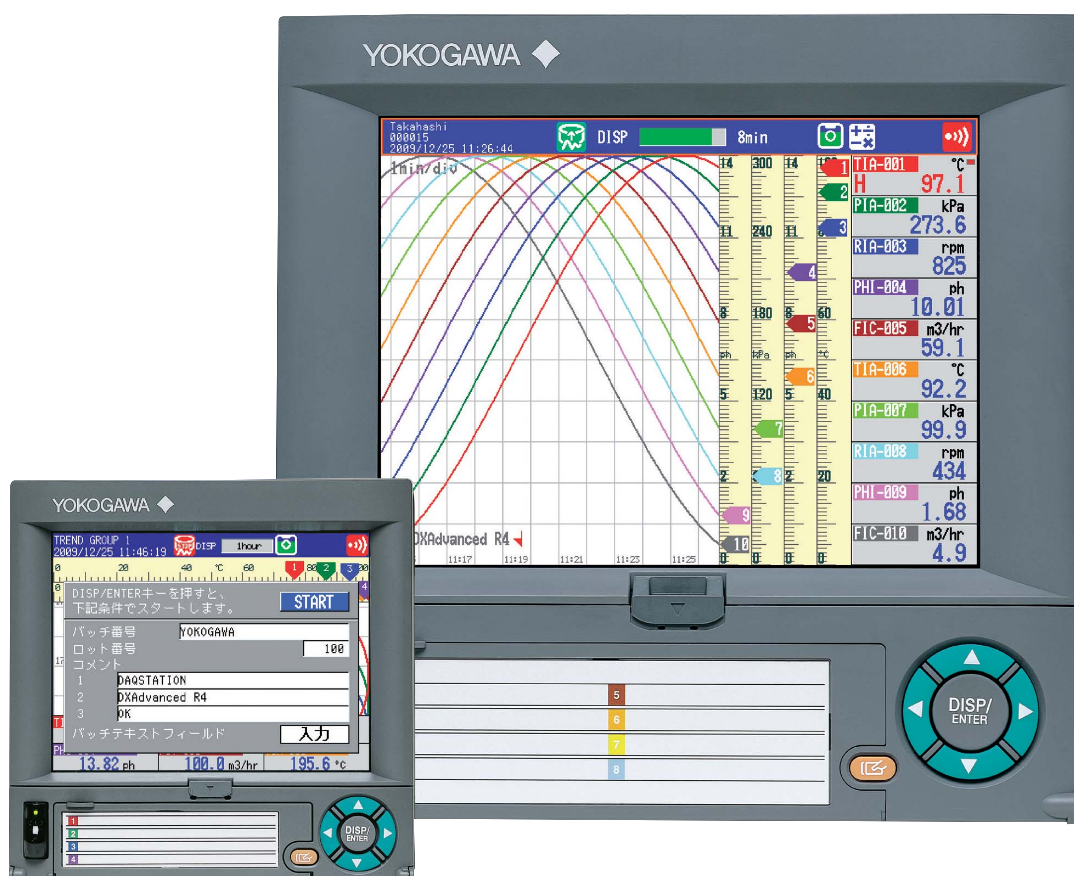
Technical Information

TI 04L41B01-03

DAQSTATION
DXAdvanced拡張セキュリティ機能
FDA 21 CFR Part 11への対応

Daqstation®



DXAdvanced® R4

DX1000 / DX2000

拡張セキュリティー機能（FDA 21 CFR Part 11対応）



YOKOGAWA ◆
横河電機株式会社

TI 04L41B01-03
2010.2.15 初版(KP)

1. 21 CFR Part 11概要

電子記録および電子署名の使用に関するFDA（米国食品医薬品局）の最終規則である21 CFR Part 11（タイトル21ー連邦規則集ーパート11）は，部分的には業界の需要に呼応しています。また，文書による事務処理の量と検閲ならびに資料庫に保管される文書の削減施策の実践を米国政府機関に対して要求したために策定された法令です。1997年8月に公布された21 CFR Part 11は，電子媒体上の記録・署名が，従来の紙による記録・手書きの署名に同等であるとFDAに承認されるための基準を規定しています。

紙ベースの文書管理と，電子記録に対する21 CFR Part 11要件の比較：

紙ベースのシステムは，無許可の変更や物理的劣化から保護された安全・確実な記録保管を要求されています。同様に，21 CFR Part 11は電子記録についても保全を保証する管理を求めています。紙ベースのシステムにおいて記録の変更が元の記載を痕跡も残らぬように消されることがあってはならないのと全く同様に，電子記録上の変更も，元のデータを改ざんする事があってはなりません。紙ベースのシステムでは，あらゆる変更はある個人に起因しますが，電子記録システムにおいての全ての変更は，変更をおこなった許可されたユーザをトレースするための監査証跡（audit trail）として記録されなければなりません。紙ベースの記録および電子記録への不正なアクセスを防止するために物理的セキュリティ管理を備えることが必要とされます。更に，不正アクセスに対する電子記録は,よりいっそうの保護のために論理的セキュリティの手順も準備しなければなりません。

記録保管についての要件は，紙ベースの記録システム／電子記録システム共に違いは無く，いずれも，所定の保管期間中は検索が可能な方式で保管される必要があります。

電子記録に適用される電子署名と電子記録への署名は，紙の記録にされた従来の手書き署名と同じ法的効力を持つことが，FDAにより認められています。従って，電子記録に適用する署名は適切に管理され，署名の偽造や他の記録への複写を確実に防止される必要があります。更に，紙の記録上で目立つように示されている署名のおかげでその署名の事実が即座に証明されるのと同様に，電子記録に署名がされていることをあらゆる定期審査や点検において検証する手段が設けられている必要があります。

また，Part 11では，対象となる全職員に対する適切なトレーニングの実施およびこれらの記録にまつわるあらゆる施策・方針の正確な文書化を保証するための管理手順を，電子記録および電子署名を利用する組織や各個人が実践することが要求されています。

21 CFR Part 11の範囲と施行

Part 11は，FDAによる単なる指導ではなく法的規制である一方，FDA規則中に明確に示された記録に対する要求事項に基づいて記録の生成／修正／管理／保管／検索あるいは転送される電子媒体上の記録にのみ適用されます。本規則は，FDAに提出される電子記録と，FDAに直接提出はされないFDAの規制要件を満足するために保存される電子記録も適用範囲としています。企業に管理される記録でもFDAの規制にも従う必要のない記録は，21 CFR Part 11にも従う必要はありません。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

2. 規制準拠のための業界サポート

ラボ・オートメーション機器の製造業を含む多種の業界が，電子記録の全ライフサイクルを通しての保全とトレーサビリティを保証するために必要な論理制御を含む，新しい改良されたシステムを開発することで，対象業界の21 CFR Part 11準拠を支援しています。横河電機(株)もこれらサポート企業のひとつであり，1915年の創業以来，横河電機(株)は最高品質のソリューションと先進の技術の工業オートメーションおよび計測分野への供給に専心し続けています。

横河電機(株)は，21 CFR Part 11の要求である強化された電子記録のセキュリティとトレーサビリティに適合することを意図した機能を備えるべく，ペーパレスレコーダDAQSTATION　DX100／DX200に対して大幅な改良をおこない，2001年にDX100PおよびDX200Pを発売しました。そして2010年にDAQSTATION第2世代となる大幅な性能アップを実現したDXAdvancedシリーズをベースに，拡張セキュリティ仕様（/AS1仕様，総称してDXAdv/AS1と呼ぶ）を発売しました。DXAdv/AS1は， 各ユーザ独自の内部手順と組み合わせて使用することにより，21 CFR Part 11の完全準拠を実現することを可能にします。本書においては，その準拠に，自動化されたシステムのみならず，内部管理手順をも必要とする要件を，「管理上の注意／手順管理」という名前の項に記述します。

DXAdv/AS1は，種々のアプリケーションから単独でデータ収集を実行するべく設計されたペーパレスレコーダであり，現在従来の記録計が使用されているあらゆる環境に効果的に組み込むことができます。この多機能なDXAdv/AS1は各々，チャンネル毎に校正可能な最大48チャンネルまでの入力，およびオプションとして最大60チャンネルの演算データを収集・統合することが可能です。記録データは，セキュリティを保たれたユーザのネットワーク上のディレクトリに転送して，DAQSTANDARDソフトウェアを使用しての更なる審査の実施や，保管／バックアップすることが可能です。更に，DAQSTANDARDソフトウェアの設定ソフトにより，適切な権限を持つ管理者がDXAdv/AS1をリモートで機器設定することも可能になりました。Web経由でリアルタイムデータを見ることができ，遠く離れた生産現場にわざわざ行くこと無しに，プロセスのより細密な監視制御が可能です。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

3. 21 CFR Part 11要件の概要と DAQSTATION DX1000/DX2000拡張セキュリティ機能（/AS1）の対応機能

論理的セキュリティ（Logical Security）

21 CFR Part 11は，FDAの要求に従い電子記録を生成／修正／管理／検索するシステムへのアクセスを，許可された個人のみに限定しなければならないと規定しています。更に，権限チェックをおこない，そのシステムにアクセスする許可された個人が，与えられたアクセス権限レベルに見合い，かつ，適切なトレーニングを受けた操作作業のみが可能であることが保証される必要があります（21 CFR 11.10(d), (g), (i)）。

ペーパレスレコーダDXAdv/AS1は，ユーザ名／ユーザ認識コード（ユーザID）／パスワードという3つまたは，ユーザ名／パスワードという2つの手段の組み合わせでセキュリティを構築し，システムへのアクセスを許可されたユーザのみに限定することが可能です。ユーザ名の重複は許されませんし，ユーザIDとパスワードの組み合わせについても同様です。権限については，データ表示アクセスのみ可能なレベルから，リモート通信・機器設定権を含む全システム管理権限を持つレベルまで，多様なアクセスレベルを定義することが可能です。DXAdv/AS1には，最大5人のシステム管理者(administrators）と同時に90人までのユーザを定義することが可能です。個々のユーザは，自分のアクセスレベルを変更することが不可能です。

このセキュリティは電子記録のライフサイクル全域にわたって保持され，対応する収集データのファイルがFTP転送，外部記憶メディア経由，または他の手段によって，より永続性のある保管場所に移された場合にも，ユーザ権限とセキュリティのデータは直接関連付けられます。

管理上の注意／手順管理

個々のユーザは，割り当てられた作業を実施するための適切なトレーニングを受けねばなりません。このトレーニングは，各ユーザ部署の明文化された方針および標準作業手順に従ったものであり，文書化されている必要があります。トレーニングには，記録計の定型化した機能と，セキュリティ等の，データが電子的な物であるために発生する付随的な要件が網羅されている必要があります。(21 CFR 11.10 (i))

ユーザ名あるいはユーザIDとパスワードの組み合わせが電子署名として使われ，署名のコピーや本人以外の使用の禁止を保証する場合には，更なるセキュリティが要求されます。ユーザIDとパスワードの組み合わせによるセキュリティの維持を保証するために，ユーザ名あるいはIDコードとパスワードは，定期的にチェックされ，呼び出され，変更されなければなりません。(21 CFR 11.200 (a) (2); 11.300 (a), (b))

DXAdv/AS1は，ユーザ名／ユーザID／パスワードの組み合わせを電子署名とする様に設定できます。システム管理者はユーザ名とユーザIDの閲覧が可能ですが，パスワードは暗号化されて保存され，システム管理者を含めた誰にも見ることができません。新たなユーザアカウントがシステム管理者によって生成されると，そのユーザレベル用に既に期限の

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

切れたパスワードが初期パスワードとして設定されます。そのアカウントへの最初のログオン時に，パスワードの即時変更が要求されます。変更後に初めてDXAdv/AS1の機能へのアクセス権を得ることができます。DXAdv/AS1では，英数字および記号6文字以上20文字以下のパスワードの入力が要求されます。パスワード中には，スペースや空白（Null）文字の入力はできません。また，大文字／小文字は区別されます。ユーザ企業のポリシー上必要であれば，システム管理者は各ユーザパスワードをそれぞれ1ヶ月，3ヶ月，または6ヶ月で期限切れとなる様に設定できます。

システムアクセスを許可されたユーザのみに限定し，各ユーザのアクセスレベルを管理する事で，記録計が定常的に使用される期間の効果的なセキュリティをもたらします。21 CFR Part 11は，更に，要求された保持期間を通して記録の容易かつ正確な検索が可能である様，記録を保護することを要求しています。この要件は，その記録の作成時のみならず，保管された電子記録に対しても，その保管期間を通して適用されます。（21 CFR 11.10（c））

FTPクライアントモード機能により，DXAdv/AS1で作成された記録を，長期または短期保管のために，セキュリティ管理されたFTPサーバ・ディレクトリに自動転送することができます。FTPサーバ・ディレクトリに対するファイルのアップロード時に，予め設定されたユーザ名とパスワードの組み合わせを必要に応じて送る機能が，DXAdv/AS1自体にあります。FTPサーバ・ディレクトリへのアクセスレベルは，適切なローカルネットワークのセキュリティポリシーによって，更に管理する事ができます。DXAdv/AS1でもDAQSTANDARDソフトウェアでも，ユーザの記録への上書きを禁止しています。データファイルは，DXAdv/AS1の外部記憶メディア（CFカード）に順次保存され，自動転送機能使用時には，FTPサーバにも保存されます。このため，サーバへのネットワーク接続が切れた際にも，データの記録は常に保管されています。接続が切れた場合には,接続回復と同時にデータが自動的にFTP転送されます。そして，ユーザの一般的な電子記録保管ポリシーに基づき，これらの記録を保持することが可能です。

管理上の注意／手順管理

DXAdv/AS1では，外部記憶媒体の残容量が不足した時に，自動的に古いファイルから上書きするFIFO (first-in-first-out)機能を備えています。もしDXAdv/AS1ローカルの記憶媒体をプライマリ(マスタ)の記憶媒体として用いる場合は，重要な電子記録の長期間の保管を確実にするため，この機能を“ Off ”にすることを推奨します。

記録のトレーサビリティと監査証跡（Audit Trails）

紙ベースのシステムにおいて記録の変更が元の記載を痕跡も残らぬように変更されることがあってはなりません。同様に，電子記録になされた変更も，元々記録されていた情報を改ざんする事があってはなりません。セキュリティ保護されたコンピュータで作成される電子記録を作成／変更／または削除するあらゆるオペレータ入力や操作の日時を自動的に記録する監査証跡がこの21 CFR Part 11によって求められています。FDAは，法規（FR vol. 62, No. 54, 3/20/97）の序文中で，「実質的に誰が，いつ，何をし，何を書き込んだかの記録」を提供することが監査証跡の目的であると述べることで，この要件を更に明確にしています。法規制による監査証跡についての要求は，ある個人に起因する動作のみを範囲とすることを目的にしているので、人為的でない計器またはソフトウェア・アプリケーションによるオペレータ入力とは無関係なバックグラウンドでの記録動作は含みません。また，

監査証跡には電子記録を変更してしまう全ての操作を記録する必要がありますが，画面切り替え等の，電子記録の内容に全く影響を与えないユーザ操作を記録する必要はありません。(21 CFR 11.10 (e))

温度指示値等の収集データに対する変更の履歴をたどることだけでなく，製造シーケンスの起動やアラーム消去等のオペレータ操作の履歴をたどることも重要です。FDAが，データの収集されたプロセスを再現し，検証する事が可能であることに関心を持っているが故に，最終的な結果を変えてしまうようないかなる変更も監査証跡によってその履歴をたどることが可能であるべきです。これには演算や校正方法、あるいは警報設定の変更も含まれます。ユーザセキュリティ設定の変更についても，データの有効性に多大な影響を及ぼす可能性があるため，その履歴をたどり変更をおこなったユーザと変更日時を明確にすることが可能であるべきです。この様なデータは，大まかにメタデータという用語で分類されます。

いかなる方法でのアクセスや変更であろうと，DXAdv/AS1は全ての警報，警報確認，エラーメッセージ（無許可アクセスの試みを含む)，および機器や演算設定の変更の記録，ならびに現在のユーザ権限レベルを複数のバイナリファイル内に保持します。これらのファイルの内容はDAQSTANDARDソフトウェアを使用して見ることができますが，ユーザやシステム管理者が変更することはできません。温度値等の収集データも横河固有のバイナリ形式で保存され，いったん保存された値を変更することはできません。ユーザがバイナリデータに直接アクセスし，変更しようとすると，ファイルはそのユーザにとって使い物にならなくなってしまいます。次に誰かがデータにアクセスしようとすると，エラーメッセージが表示され，データは変更されてしまったためファイルの内容を見ることができないと通知されます。

管理上の注意／手順管理

全データの正確なコピーが安全に管理され，要求された保管期間を通して検索可能であることを保証するべく，バックアップと保管の手順を策定し遵守せねばなりません。(21 CFR 11.10 (b), (c))

監査証跡はコピー可能であり，かつ，該当電子記録の要求された保管期間中は審査可能でなければなりません。(21 CFR 11.10 (e))

DXAdv/AS1により作成された個々のログは変更後に作成された次のデータファイルにリンクされます。これらのログは，元のデータファイルがコピーされるたびに自動的にコピーされ，FTPサーバに転送されて関連データファイルと共に長期保存されます。

検　証（バリデーション）

電子記録の作成，修正，管理に使用されるシステムは，その正確性，信頼性，整合性のある意図した性能，および，無効なまたは変更された記録を識別する能力を保証するために検証しなければなりません。(21 CFR 11.10 (a))

大部分の検証試験を工場で実施することが可能ではあるものの，FDAの要求に完全に対応するためには，システムの実際の動作環境においてシステムの検証を実施する必要があります。故に，いかなる機器メーカも，その供給システムがFDAの規定する環境での使用に

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

つき完全に検証済みであると，証明することはできません。しかし，個々のユーザは，あらかじめ決められたDXAdv/AS1が持つ機能を選択するのみですから，ユーザ固有の機能要件を満たすべく，個々のユーザが設置テスト，設定テストならびに機能テストの認定規約として完成させることが可能なものを用意することができます。横河は，エンドユーザ自身の運転方針や手順と組み合わせて使用することにより，本システムの検証要求を満足することの可能な設置テスト，設定テストならびに機能テストをバリデーションドキュメントとして別売しています。

記録の維持

21 CFR Part 11では，保存期間を通した電子記録の保護により，正確で素早い検索を可能とするよう要求しています。更に，人間にもコンピュータにも可読であり、またFDAによる検査，審査，複写に適したコピーが作成可能でなければなりません。元の記録作成の一因となったプロセスを仮想的に再現することを可能とするため，コピーは正確で完全なものである必要があります。（21 CFR 11.10 (b)）

この要件の鍵は，メタデータのコンセプト，換言すれば，データについてのデータです。メタデータとは，収集された結果または測定結果に加え，収集データの収集環境を決定するデータです。DXAdv/AS1の設定においては，データ収集に用いる実際のDXAdv/AS1の機種やモデル，入力チャンネル設定，入力値補正設定，警報設定，演算チャンネルの演算プログラム，ユーザアクセスレベル，測定単位，熱電対タイプ（これらは総称してシステム設定と呼ばれるデータです），そして記録開始,停止の日時が含まれますが，決してこれらに留まりません。メタデータの全ては専用の複数の機器設定（コンフィグレーション）ファイルに保存されていて，運転開始時に次のデータファイル内にコピーされます。これがDXAdv/AS1の電子的監査証跡データとなります。これらの情報はバッチデータファイルとともに自動的に保存されるため，バッチデータが維持されているとメタデータも当然維持されます。

FTPクライアントモード機能の使用により，DXAdv/AS1のデータを安全に維持できます。DXAdv/AS1はデータファイルを自動的にセキュリティ管理されたネットワークサーバに転送することが可能です。プライマリサーバ・セカンダリサーバが指定可能で，一次サーバとの接続が切れた時，ファイルは自動的に二次サーバに送られます。FTPクライアントモード使用時には，データファイル（全監査証跡データを含む）は外部記憶メディア（CFカード）とサーバに同時に保存されます。これらのどちらの記憶場所も，マスターユーザコピー，バックアップ，最終保管場所として選択することが可能です。以下に，DXAdv/AS1の多様な使用方法を述べます。

用法1：記録ストップ時（データまたはバッチデータファイルの記録終了）にデータを外部記憶媒体に保存し，同時にバックアップコピーをFTPでネットワークサーバに送る様にDXAdv/AS1を設定します。外部記憶メディアに保存したファイルには，DAQSTANDARDソフトウェアを使って，電子署名を適用することが可能です。いかなる状況下でも，DXAdv/AS1本体とDAQSTANDARDソフトウェア使用時では，同一のアクセスセキュリティが適用されます。DXAdv/AS1本体で媒体に保存されたデータが変更される度に，更新されたバックアップファイルがFTPでサーバに送られます。これらのバックアップファイルはユーザ企業の確立されたネットワーク・バックアップ手順に従い維持保管することが可能です。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

管理上の注意／手順管理

バッチモードでデータ収集し，1バッチのデータが複数ファイルに格納される場合には，DAQSTANDARDソフトウェアを使わないと電子署名ができません。詳細は，本書の「DXAdv/AS1における電子署名の使用」項に後述します。

用法2：DXAdv/AS1単体を完全に独立して使用し，FTP転送機能を使用しません。全データは内部メモリおよび外部記憶メディアにのみ保存され，内部メモリがマスターの保管場所であり，外部記憶メディアはマスターのコピーの保管場所ともなります。内部メモリのファイルを適宜検索して，DXAdv/AS1本体で，後で記録を審査し，署名することができます。外部記憶メディア上のファイルは，DAQSTANDARDソフトウェアを使い，後で記録を審査し，署名することができます。この用法では，各データファイル毎に，単一の作業用コピーが使用可能であり，全ての変更は同一のファイルにされます。バックアップは，ユーザの定型化したバックアップ方針に従って作成することができます。

管理上の注意／手順管理

バックアップや保管記録の作成手順等の手順書は，全電子記録が，その要求される記録保管期間を通して適切に保護されることを保証するように策定されていなければなりません。（21 CFR 11.10（c））

DXAdv/AS1およびDAQSTANDARDソフトウェアにより維持される記録は，バックアップや保管が容易な形式で媒体に保存されています。記録は，アクセス規制されたネットワークディレクトリまたは他の場所に確実に保存され，ユーザの定型化した手順に則り保管され，検査や監督官のためのコピー作成が必要な時に即入手可能となる様にします。DXAdv/AS1が作成し保存したデータは，DXAdv/AS1上で，あるいはDAQSTANDARDソフトウェアを使ってのみ見ることができます。

管理上の注意／手順管理

ユーザの変更管理／バックアップ／保管／事故修復方針には， DXAdv/AS1のデータファイルの取り扱い，および，使用する場合にはDAQSTANDARDソフトウェアの使用についての方針も必ず含まれている必要があります。

オープンなシステムのより確実な管理

21 CFR Part11では，オープンおよびクローズドシステムの2つのデータ保管システムのカテゴリーが認識されています。クローズドシステムとは，システム上で管理される電子記録の内容に責任を持つ同じ人達によりシステムアクセスが管理されるシステムを持つ環境と定義されます。オープンシステムとは，システム上で管理される電子記録の内容に責任を持つ人達以外の人達によりシステムアクセスが管理されるシステムを持つ環境と定義されます。クローズドシステムの例としては，単体のPCや企業のローカルネットワークが含まれます。オープンシステムの例としては，外部のインターネットサービスプロバイダーを通じてアクセスされる可能性のあるシステムがあります。オープンシステムを通じてデータが送られた際のデータの完全性と機密性に対するリスクの増大のため，21 CFR Part11は

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

文書の暗号化やデジタル署名などを含むさらなるデータに対する追加管理を要求しています。

DXAdv/AS1は単体で独立した計器として機能し，ユーザによるリモートアクセスを禁止できます。 DXAdv/AS1自身以外のいずれの場所からもそのデータを収集することはできません。MicrosoftのInternet Explorerを使ってDXAdv/AS1の状態をリモートで見ることが可能ですが，同じ方法で電子データを変更することはできません。DAQSTANDARDソフトウェアの提供するリモート機器設定機能は，ユーザ企業におけるローカルネットワークのパラメータ設定の範囲内でしか機能しません。つまり，システムアクセスは，DXAdv/AS1の電子記録の内容に責任のある同じ人達によって常時管理されるので，21 CFR Part 11がオープンなシステムに求める，より確実なセキュリティ要件はDXAdv/AS1に適用されません。充分なアクセス権を持つユーザであれば，DAQSTANDARDソフトウェアを使用して， FTPでネットワークディレクトリに転送されたデータにアクセスして審査や署名をすることができます。DAQSTANDARDソフトウェアは，DAQSTANDARDを使うPC個々にインストールしなければなりません。ユーザネットワークへのアクセスが企業により規制される場合には，DXAdv/AS1に連結されたオープンなシステムに関連した問題は発生しません。（21 CFR 11.30）

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

4. 電子署名のセキュリティと明示要件

21 CFR Part 11では，電子記録に適用される電子署名に対する基準を規定し，この基準に適合した電子署名が紙の記録にされた手書きの署名と法的に同等であると見なされるのに必要な特性を持つことを保証しています。従来のデータ操作手法による電子署名の複製や偽造を確実に防ぐための対策が実施されねばなりません。更に，電子署名が本人以外の誰にも使われること無く，明確にたった一人の個人を示すものである事を保証する論理的セキュリティ機能が確立している必要があります。（21 CFR 11.70; 11.200 (a) (2), (3); 11.300 (a)）

管理上の注意／手順管理

ユーザは，電子署名の使用開始前に，署名された申告書をFDAに提出し，自身のシステム内で使用する電子署名が従来の手書き署名と同等の法的拘束力を有する物であることを証明せねばなりません。この証明申告書は紙の書類として提出されねばならず，総括して組織全体の全ての電子署名について述べたもので構いませんが，FDAから要求があった時には，補足的な個々の電子署名の証明を提出せねばなりません。（21 CFR 11.100 (c)）

電子署名に要求される管理は，適用される署名の種類により異なります。ユーザIDとパスワードの組み合わせ等，キーをたたく順序のみに拠る署名では，その署名が許可されたユーザのみに連続使用可能であることを確実にする定期的なパスワード失効等の管理が必要です。キー入力と機器または何らかのしるし（トークン）を用いる電子署名では，改ざんの事実が無いことを保証するための紛失管理制策と定期的な実績検査が必要です。更に，これらの署名は，使用されるトークンやカードを機械のスロットに通して読ませるという類の，単一の因子に拠るものであることは許されません。パスワード入力その他の作業で、万一トークンが盗難された場合にも無許可ユーザの使用を防ぐ様な付加的な手段と組み合わされなければなりません。指紋や音声スキャン等のバイオメトリクス（生物測定学）を利用した電子署名は，明らかに最も安全な署名形式です。しかし，これらの方式は，各署名の真の使用者以外，何人たりとも使用することが不可能であることを確実にするべく慎重に設計されねばなりません。この種の電子署名は，全面的に21 CFR Part 11に遵守し秘匿（ヒトク）対策がとられていれば，パスワード等の二次的な確認は不要です。（21 CFR 11.300 (b), (c); 11.200 (b)）

DXAdv/AS1における電子署名の使用

DXAdv/AS1記録計では，ユーザ名，ユーザIDそしてパスワードを組み合わせた電子署名の使用が可能です。3種までの電子署名を各データファイルに添付することができ，機器設定時に個々のユーザには各々署名場所（署名1／署名2／署名3／または署名権無し）が割り付けられます。各ユーザは，記録上の割り付けられた場所に署名が未記入であった場合にのみ，署名することができます。システム管理者は，他人の署名が記入されていない署名場所であれば，どこでも署名することが可能です。

DXAdv/AS1はバッチモード／連続モードのいずれのモードでも動作してデータ収集できます。バッチモードでは，単一のファイルまたはバッチ実績を作成し，その記録長は開始／停止操作によって決定します。このモードでは，DXAdv/AS1本体で直接署名を記入することができますし，後でDAQSTANDARDソフトウェアを使ってコンピュータ上で記録を確認する際にも署名が可能です。しかし，バッチが長時間におよび，ひとつにバッチ実

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

績が順次保存された複数ファイルにより構成される場合もあり得ます。この場合には，後でDAQSTANDARDソフトウェアを使って記録を確認する際にのみ署名が可能です。DAQSTANDARDソフトウェアは自動的にこれらの複数バッチファイルを結合し，署名情報をバッチ実績中の各ファイルに適用します。

連続モードでは，個々のデータファイルは他のいかなる存在とも無関係の孤立した存在です。署名はDXAdv/AS1本体でも，DAQSTANDARDソフトウェアを使って記入することが可能です。連続モードで収集したデータに添付する電子署名は，バッチ全体ではなく，ひとつのデータファイルにのみ適用されます。また，DAQSTANDARDソフトウェアにより連結表示された複数のデータファイルに電子署名を記入することも可能です。

電子署名全般に対する共通要件

個々の電子署名は一義的に単一の個人を示すものであり，これを再使用したり,後に他の人に割り付けることは許されません。(21 CFR 11.200 (a) (2), (b))

DXAdv/AS1には，ユーザIDの組み合わせで同時に5人までのシステム管理者と90人までの一般ユーザが登録可能です。ユーザ名および/あるいはユーザIDとパスワードの組合せが重複することはできません。またユーザ名および／あるいはユーザIDとパスワードの組み合わせを複製することはできませんので，個々の電子署名から一義的に単一の個人を突き止めることが可能です。

管理上の注意／手順管理

電子署名を使用するユーザに，自分たちの電子署名のもとに開始された操作に対する責任を持たせるべく，明文化された方針が設けられている必要があります。社内トレーニングでは，他人の認識情報の使用およびIDとパスワードの組み合わせの他人との共用により起こり得る結果に重きを置くべきです。更に，各ユーザに電子署名の使用許可を与える前に各ユーザの個人情報を照合することが企業に要求されます。この手順は殆どの人材方針に容易に取り入れることが可能です。(21 CFR 11.10 (j); 11.100 (b))

バイオメトリクスを利用しない電子署名は，最低2つの異質な構成要素を用いねばなりません。例えば，ユーザIDとパスワードの組み合わせによる電子署名や，磁気カードとパスワードの組み合わせによる電子署名等です。これらの構成要素のひとつは，正当なユーザ以外が実行可能であってはいけません。あるユーザが一回の規制された連続アクセスセッション中に何度も電子署名を使う場合には，最初の署名時に電子署名の全構成要素が使用されねばなりません。同じセッション中の二回目以降の署名では，個人のみが実行可能な構成要素が使用さなければなりません。一回の規制された連続アクセスセッション中に，二回以上署名がされない場合には，電子署名の個々の構成要素をセッションの度に使う必要があります。(21 CFR 11.200 (a))

DXAdv/AS1は，最も厳しいレベルのセキュリティとして，ユーザ名／ユーザID／パスワードの3要素の組み合わせを用いて定常的なユーザアクセスを許可します。ユーザが自分のユーザIDとパスワードを正しく入力すると，電子署名処理により，ユーザの名前が自動的に記録されます。パスワード要素は暗号化されて保存され誰にも見ることができません。個々の電子署名では，ユーザIDとパスワードの再入力がユーザに要求されますので，DXAdv/AS1使用時の規制されたアクセスが連続かあるいは非連続かによる問題が生じま

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

せん。DAQSTANDARDソフトウェアを使った署名適用も同一の要素と規制が含まれます。

電子署名は，正当な持ち主以外の人物による個人電子署名の使用の試みには，2人以上の個人の協力を必要とする様に管理され実践されねばなりません。(21 CFR 11.200 (a) (3))

ユーザ識別のパスワード要素は暗号化された形式で保存され，システム管理者を含む誰にも見ることができません。

> **管理上の注意／手順管理**
>
> 横河ではDXAdv/AS1本体の英数字キーに加え，更に簡単かつ安全確実なパスワード／ユーザID／コメント文字列入力を可能にする簡易入力オプション(リモートコントロール)を発売しています。また，文字列の入力にUSBキーボードを使用することもできます。パスワードを使うあらゆるシステムと同様に，各ユーザは，他人が見ている時に自分の個人機密コードを入力しない様注意する必要があります。

署名の明示

活字体で書かれた署名者の名前，署名日時，および署名することの意味が，人間が可読な形式の電子記録の一部として含まれていなければなりません。これには，紙面上および電子的での表示の両方を含みます。いかなる一般的な記録操作手法を使っても電子署名を削除，コピー，転写することができないように電子署名は各々の該当する電子記録とリンクされていなければなりません。（21 CFR 11.50, 70）

登録されているユーザは，あるデータファイルに署名行為を行う前に，DXAdv/AS1またはDAQSTANDARDソフトウェアにログインする必要があります。ユーザ名は，初めに入力されている通りに，自動的に電子署名に適用されます。署名日時は署名と共に自動的に保存されます。DXAdv/AS1内の日時設定は登録されたシステム管理者および許可された一般ユーザのみが変更可能であり，その他の一般ユーザには変更不可です。あるユーザがDXAdv/AS1のデータファイルに電子的な署名をする時には，署名の意味として“ Pass ”(合格）または“ Fail ”(不合格）のいずれかを選択するように要求されます。このとき，英数字/カナキーを使って付加コメントを入力することもできます。DXAdv/AS1が作成した記録に適用される電子署名は，添付後に削除することができません。DXAdv/AS1のデータファイルは固有のバイナリ形式で保存されているため，作成後に一般的な方法で修正することができません。電子署名も全く同様です。実際の署名と全ての関連データはDXAdv/AS1本体で，またはDAQSTANDARDソフトウェアを使って見ることができます。

> **管理上の注意／手順管理**
>
> DXAdv/AS1環境における電子署名を21 CFR Part 11に完全に準拠させるためには，DXAdv/AS1へのアクセスを許可するためにユーザを登録する際，ユーザ名をフルネームでユーザ名フィールドに入力する必要があります。ユーザ名フィールドそのものには最低入力文字数が規定されていませんので，この要件(ユーザ名のフルネーム入力)が常に確実に遵守されるよう，ユーザの手順書のひとつに規定される必要があります。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

認識コードとパスワードの特殊管理

電子署名に使われる認識コード（ユーザ名およびユーザID）とパスワードは，機密保護の継続を確実にするため定期的なチェック，呼び出し，あるいは改訂が必要です。更に，使用中のいかなる不正な試みも確実に検知，報告，防止するトランザクションの保護も必要です。単に不正使用中の処理を検知して報告するだけでは不十分です。他人を詐称することにより，記録にアクセスし署名することも防止しなければなりません。（21 CFR 11.300 (b), (d)）

DXAdv/AS1では，ユーザパスワードは1ヶ月，3ヶ月，あるいは6ヶ月で期限切れになるように設定可能です。この期間を超えて，同じパスワードを再入力することはできません。いかなるユーザも，登録されたユーザ名とパスワードの組み合わせを入力してDXAdv/AS1にログインしない限り，DXAdv/AS1の記録に電子的な署名をすることができません。ユーザは，ログイン時にユーザ名とパスワードの組み合わせを正しく入力するよう3回もしくは5回まで試みることができます。誤った入力を3回もしくは5回繰り返した場合には，そのユーザのアクセス権は失効され，システム設定によっては通知が送られます。適切な調査の後に，システム管理者は警告メッセージを確認し，該当ユーザのアクセス権を再設定し，実際の署名の持ち主に記録計の使用と電子的な記録への署名を許可することができます。

管理上の注意／手順管理

定期的なパスワード失効は，明文化された手順中に規定され，その規定はDXAdv/AS1のユーザ設定にも反映される必要があります。

実際の署名適用レベルには，これ以上のセキュリティが施されています。ある記録に署名しようとする不穏当な試みが3回もしくは5回おこなわれると，そのユーザは該当記録に対する署名権限を永久に失います。このとき，警告メッセージがDXAdv/AS1の画面に現れます。システム管理者は，その後のデータとDXAdv/AS1の機能に対するこのユーザのアクセス権限を復活させることができますが，該当バッチに対するユーザ権限を復活させることはできません。このセキュリティにより，DXAdv/AS1およびDAQSTANDARDソフトウェア環境のいずれにおいても，ユーザの署名情報に対する不正変更は防止されています。このユーザが該当データファイルに署名することがどうしても必要な場合には，レポートを印字すれば誰でも手書きで署名が可能です。

管理上の注意／手順管理

最低2名のシステム管理者を常に登録しておくべきです。あるシステム管理者のユーザ情報を使った不当な試みが検知されると，一般ユーザ同様に，そのシステム管理者のアクセス権限が失効されてしまいます。この時，他にシステム管理者が登録されていない場合には，それ以降の該当DXAdv/AS1への管理者権限を必要とするアクセスは全て不可能になります。

使用中の不正な試みについての全ての通知と，誰がそれらのメッセージを確認しリセットしたかの永続的記録は，DXAdv/AS1の監査証跡記録の一部として維持されます。したがって，ユーザアクセスまたは署名適用に関する疑問が生じた場合に，システム管理者はそのデー タを綿密に調べ，必要な是正処置を決定することが可能です。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

5.　その他の手順管理

ドキュメンテーション

完全なシステム文書とは，標準操作手順，仕様および検証書類，トレーニング記録，およびDXAdv/AS1が監視するプロセスに適用される企業方針を記したその他の書類を含みます。このドキュメントは紙ベースでも，または電子的な文書であっても構いません。媒体に関わらず，システム文書全体の適切な管理が確立されていて，配布の管理と改訂・変更管理手順の遵守が確実にされていることが必要です。改訂・変更管理手順には，変更を時系列に記録する監査証跡も含まれている必要があります。（21 CFR 11.10 (k)）
実際に実施される管理は，各企業固有の文書システムに依存します。文書は，電子形式であれば頻繁に保存され変更されますが，電子文書／紙文書のいずれであっても日常的にアクセスされますので，管理は両方の形式の媒体について実施される必要があります。電子記録の定義に該当するあらゆる関連資料は，21 CFR Part11に準拠した方法で維持されねばなりません。電子記録システムに関する紙文書の利用と改訂もまた，Part 11.10 (k)項に従って管理されねばなりません。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart B-Electronic Records（サブパートB：電子記録） *Subpart B, §11.10 Controls for closed systems.* →*"Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."*（クローズドシステムの管理：クローズドシステムを使って電子記録の作成, 修正, 保存,転送を行う者は, 電子記録の信頼性, 完全性及び, 必要に応じては機密性を確保でき，且つ，署名者がその署名した記録を真正のものでは無いと容易に否認することを確実に不可能とするような手順ならびに管理方法を用いる。）	○		DX1000/DX2000拡張セキュリティ仕様（以降DXAdv/AS1と総称する）は，システムアクセスを指定されたユーザのみに限定する手段を持ち，独自のバイナリ形式でデータを記憶し，高レベルのセキュリティを持つ。DXAdv/AS1を介して保存されたデータを変更可能な手段は一切無い。 DAQSTANDARDソフトウェアは，個々のデータファイルにCRCチェックを行い，データファイルが変更されていた場合，ユーザに知らせる。 DXAdv/AS1またはDAQSTANDARDソフトウェアで付加される電子署名は，削除不可能である。ユーザアクセス権限の管理により，ユーザが自分自身以外の電子署名を使うことができない。
Subpart B, §11.10 (a) →*"Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."*（正確性，信頼性，整合性のある意図した性能，および，無効なまたは変更された記録を識別する能力を確保するためのシステム検証）	○		アクセサリで設置，設定テストおよび機能テストパッケージが提供され，エンドユーザ自身の操作ポリシーおよび操作手順と組み合わせて使用することにより，本システムの検証要求を満足することができる。
Subpart B, §11.10 (b). →*"The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency."*（人間にもコンピュータにも可読な，そして当局による検査，審査，複写に適した正確且つ完全なコピーが作成可能であること）	○		DXAdv/AS1の表示データファイルおよびイベントデータファイルは横河独自のバイナリ形式で保存されている。これらのファイルには監査証跡（audit trail）データも含まれている。これらのファイルのデータは，横河のViewerソフトウェアを用いて人間が読める形で表示および印字できる。これらのファイルは,バックアップ，保管，検査，および確認のためにコピーすることが容易に可能である。
Subpart B, §11.10 (c). →*"Protection of records to enable their accurate and ready retrieval throughout the records retention period."*（記録の保持期間を通した，記録の容易かつ正確な検索を可能とするための記録の保護）	○		DXAdv/AS1の記憶媒体は長期保存検索目的で保管することが可能であるし,あるいは，ファイルをCD-ROM等の他の長期保管媒体にコピーすることも可能である。Viewerソフトウェアは，データファイルと共にCD-ROMに保存することが可能であり,そのファイルを見ることが可能なソフトウェアを確実に長期間維持できる。DXAdv/AS1およびDAQSTANDARDソフトウェアを介して保存されたデータを変更する手段は一切無い。
Subpart B, §11.10 (d). →*"Limiting system access to authorized individuals."*（システムアクセスを許可された個人に限定）	○		DXAdv/AS1はユーザ名，ユーザID，およびパスワードを用いた3レベルのアクセス認証機能をサポートしている。 5人までのシステム管理者（Administrators）と90人までの一般ユーザ（Users）を設定することができる。システム管理者はあらゆる機能とメニューが利用可能である。ユーザのアクセス権限は，システム管理者により詳細定義することが可能である。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart B, §11.10 (e). → “ Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded Information. Such audit trail documentation shall be retained for a period for at least as long as that required for the subject electronic records and shall be available for agency review and copying.”（電子記録を作成，修正，または削除するオペレータ入力／操作の日付と時間を単独で記録するための，セキュリティ保護され，コンピュータにより作成された，時刻印付きの監査証跡の使用。電子記録上の変更は，元のデータを隠蔽する事があってはならない。その様な監査証跡のドキュメンテーションは，最低でも当該の電子記録に要求される保持期間中は，保持されねばならず，当局による審査と複写が可能であらねばならない。）	○		DXAdv/AS1は全ての警報，警報確認，エラーメッセージ（不正アクセスの試みを含む），および機器や演算設定の変更，ならびに現在のユーザ権限レベルの記録を複数のバイナリファイル内に保持している。これらのファイルの内容はDAQSTANDARDソフトウェアを使用して見ることが可能であるが，ユーザやシステム管理者が変更することはできない。 DXAdv/AS1により生成された個々のログは変更後に生成された次のデータファイルにリンクされる。これらのログは，元のデータファイルがコピーされるたびに自動的にコピーされ，FTPサーバに転送されて関連データファイルと共に長期保存される。
Subpart B, §11.10 (f). → “Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.”（ステップやイベントの許された順序付けを徹底するためのシステム作動状態検査の使用）	○		DXAdv/AS1では，収集が停止した後でのみ，データを確認して電子署名することが可能である。 １バッチのデータが複数ファイルに格納される場合には，そのバッチのデータを持つ全ファイルが存在しない限り，そのデータに電子署名することはできない。
Subpart B, §11.10 (g). → “Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.”（システムの使用，記録への電子署名，操作またはコンピュータシステム入／出力機器へのアクセス，記録の変更，および手元での操作が，許可された個人のみ可能であることを確実にするための権限チェックの使用）	○		DXAdv/AS1はユーザ名およびパスワードを用いた2レベル，あるいはユーザ名，ユーザID，およびパスワードを用いた3レベルのアクセス認証機能をサポートしている。 電子署名付加時に，同一の権限チェックが適用される。
Subpart B, §11.10 (h). → “Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source data input or operational instruction.”（必要に応じて元のデータ入力または操作指示の妥当性を決定するための，ターミナル等機器のチェックの使用）	○		DXAdv/AS1は，ローカル（局所の）ユーザインタフェースで機器設定可能な独立機器として機能する。 DXAdv/AS1の収集データは，ユーザIDとパスワードの検証等の利用可能なネットワークセキュリティ機能を組み込み，セキュリティ保護された片道通行のインタフェースを介してネットワークディレクトリへ送ることができる。
Subpart B, §11.10 (i). → “Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.”（電子記録／電子署名システムを開発，管理，または使用する者が，彼／彼女達に割り当てられた作業を実行するための教育およびトレーニングを受け，経験のあることを決定）	非該当		トレーニングとユーザ適格性確認の文書化は,個々の組織に責任がある。横河は，ユーザ企業自身のトレーニング手順書に織り込むことが可能な，DXAdv/AS1とDAQSTANDARDソフトウェア個々の取扱説明書を提供する。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	要求に対応？		コメント
	対応	未対応	
Subpart B, §11.10 (j). →*"The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification."*（記録と署名の偽造を防ぐため，電子署名の結果生じた行為，行動に対する責任は，その署名を行った個人に帰することを明確にした，文書化されたポリシーの確立と厳守）	非該当		電子署名の結果生じた行為，行動に対する責任は，その署名を行った個人に帰することとする文書化されたポリシーは，個々のユーザ企業に責任がある。DXAdv/AS1では，各企業の内部手順書と組み合わせることにより，この規約への適合を容易にするであろうセキュリティ保護された署名の使用を選択する自由を提供している。
Subpart B, §11.10 (k). →*"Use of appropriate controls over systems documentation including:"* *1) "Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance."* *2) "Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation."* （システム文書全体の適切な管理。この管理には，1）システム操作と保守に関する文書の配布，アクセス，使用の適当な管理ならびに，2）システム文書の準備および変更を時系列に記録する監査証跡を維持するための改訂・変更管理手順，を含む）	非該当		ドキュメントの準備手順と管理手順は個々のユーザ企業にて確立されねばならない。
Subpart B, §11.30. Controls for open systems. →*"Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 、11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality."*（オープンシステムの管理：オープンシステムを使って電子記録の作成，修正，保存，転送を行う者は，電子記録が作成された時点から受領時点までの信頼性，完全性及び，必要に応じては機密性を確保できるような手順ならびに管理方法を用いる。この様な手順ならびに管理方法には，§11.10で定めたクローズドシステムでの手順と管理に加えて，オープンシステムにおける記録の信頼性，完全性，機密性を保証するための追加手順としての文書暗号化や適切なデジタル署名が含まれる。）	非該当		DXAdv/AS1はクローズドシステムである。記録へのアクセスは，その記録内容に責任がある者自身により管理される。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart B, §11.50. Signature manifestations. a) *"Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:"* 1) *"The printed name of the signer;"* 2) *"The date and time when the signature was executed; and"* 3) *"The meaning (such as review, approval, respons-ibility, or authorship) associated with the signature."* b) *"The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)."* （署名の明示：a)署名された電子記録は，署名に関する次の事項を明確に示す情報を含むこと－1)活字体で書かれた署名者の氏名，2)署名のなされた日時，3)署名の持つ意味〔審査，承認，責任，または著者であること等〕。b) 上記(a)(1)，(a)(2)，(a)(3)に示された事項は，電子記録と同じ管理の対象であり，何らかの人間可読な形式の電子記録〔電子表示または印字〕の一部として含まれること。）	○		電子署名が付加されると，ユーザ名と署名日時が，その署名された記録に自動的にリンクされる。ユーザは，各署名について，Pass／Fail（合／否）のいずれかを選択でき，テキストメッセージを入力することができる。 電子署名は記録とリンクされ，削除は不可能である。署名に関わる全情報はDXAdv/AS1本体及び，DAQSTANDARDソフトウェアを介し，電子表示あるいは印字出力上で確認することが可能である。
Subpart B, §11.70. Signature/record linking →*"Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means."*（署名／記録のリンク：電子記録になされる電子署名および手書きの署名は，該当電子記録にリンクされ，その署名が一般的な手段によって切り取られ，コピーされ，またあるいは電子記録偽造のために転写されることの無いことを確実にすること。）	○		電子署名は，当該データ群に恒久的にリンクされる。個々のファイルには3つまでの電子署名を記入することが可能である。 署名が，独自のバイナリ形式で保存されたデータファイルと恒久的に対応付けられているため，いかなる電子署名も，削除あるいはコピーすることが不可能である。
Subpart C-Electronic Signatures（サブパートC：電子記録） *Subpart C, §11.100 (a). General requirements* →*"Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else."*（概括的要求：個々の電子署名は個人に特有のものであり，該当者以外に再使用，再割り当てされることがあってはならない。）	○		DXAdv/AS1では，電子署名使用時にもログイン時と同じ権限レベルを適用する。つまり，電子署名は常に，一意のユーザ名，ID，パスワードの組み合わせに基づく。
Subpart C, §11.100 (b). →*"Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual."*（個人の電子署名あるいは電子署名の一構成要素を設定，割り付け，認定，またあるいは認可に先立ち，組織はその個人の個人情報を検証すること。）	非該当		これらの管理は，個々のユーザ企業が履行せねばならない。
Subpart C, §11.100 (c). →*"Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures."*（電子署名の使用者は，使用と同時またはそれに先立ち，自身のシステム内で1997年8月20日以降に使用する電子署名が従来の手書き署名と同等の法的拘束力を有する物であることを当局に対して証明すること。）	非該当		この証明書は，個々のユーザ企業によってFDAに提出されねばならない。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart C, §11.100 (1). →*“The certification shall be submitted in paper form with a traditional handwritten signature, to the Office of Regional Operations (HFC-100).”*（証明書は紙の書類として手書きの署名付きで地方運営局［HFC-100］に提出する。）	非該当		この証明書は，個々のユーザ企業によってFDAに提出されねばならない。
Subpart C, §11.100 (2). →*“Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer*ʼ*s handwritten signature.”*（電子署名の使用者は，FDAの要求に応じ，上記証明の補足として，ある特定の電子署名が従来の手書き署名と同等の法的拘束力を有する物であることの証明あるいは証拠を提供せねばならない。）	非該当		この証明書は，個々のユーザ企業によってFDAに提出されねばならない。
Subpart C, §11.200. Electronic signature components and controls. *a) “Electronic signatures that are not based upon biometrics shall:* *1) “Employ at least two distinct identification components such as an identification code and password.”* *i) “When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic use components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.”* *ii) “When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.”* （電子署名構成要素と電子署名管理：バイオメトリクスを利用しない電子署名は，ユーザIDとパスワードの組み合わせ等の，最低2つの異質な認識要素を用いねばならない。ある個人が，一回の規制された連続システムアクセス期間中に何度も電子署名を使う場合には，最初の署名時に電子署名の全構成要素を使用すること。同期間中の二回目以降の署名では，その個人のみが実行可能かつ，その個人にのみ使用されるよう意図された，最低一種の構成要素を使用すること。一回の規制された連続システムアクセス期間中ではなく，二回以上の署名をする場合には，電子署名の全構成要素を署名の度に使うこと。）	○		DXAdv/AS1は，ユーザ名／パスワードという2つの認識要素の組み合わせ，またはユーザ名／ユーザID／パスワードという3つの認識要素の組み合わせが使用可能である。これらの組み合わせは，重複が許されない。ユーザは，毎回の署名時に，全ての電子署名構成要素を入力することが求められる。
Subpart C, §11.200. continued *2) “Be used only with their genuine owners: and”* *3) “Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.* *b) “Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.”* （§11.200, (a)の続き…バイオメトリクスを利用しない電子署名は，本来の署名者のみが使用すること，ならびに，本来の署名者に代わり誰かが電子署名を使用する場合は，二人あるいはそれ以上の人間の協力が必要となるような仕組みをつくり，そのように実施しなければならない。） （バイオメトリクスを利用した電子署名は，本来の署名者以外が使用できぬことを確実にするよう設計すること。）	○		他のユーザはユーザIDとパスワードを見ることはできない。パスワードは暗号化されて保存されており，システム管理者にさえも見ることができない。システム管理者にできるのは初期値に再設定する事だけである。初期値は既に期限の切れたパスワードであり，最初のログイン時にパスワードの即時変更をしない限り，いかなるDXAdv/AS1の操作も行うことはできない。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart C, §11.300. Controls for identification codes/passwords. → *"Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:"* *a) "Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password."* （IDコード／パスワードの管理：IDコードをパスワードと組み合わせて用いる電子書名の使用者は，それらのセキュリティと完全性を確保するべく管理を実行すること。そのような管理とは，2人の個人が決して同じ組み合わせを持たない，という個々の組み合わされたIDコードとパスワードの一意性の維持を含む。）	○		DXAdv/AS1では，ユーザ名とパスワード，あるいはユーザIDとパスワードの組み合わせの重複は許されない。
Subpart C, §11. 300. Controls for identification codes/passwords. (Cont.) *b) "Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)."*（§11. 300の続き…そのような管理とは，IDコードとパスワードの発行が定期的にチェックされ，使用不能にされ，改訂されることの徹底［パスワード使用期間チェック等］を含む。）	○		パスワードは，1，3，または6ヶ月で自動的に期限切れするよう設定可能である。 この機能はOFFにも設定可能である。
Subpart C, §11. 300. Controls for identification codes/passwords. (Cont.) *c) "Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls."*（§11. 300の続き…そのような管理とは，遺失，盗難，紛失した，またあるいは損なわれた可能性のある，IDコードまたはパスワード情報を記録している，あるいは生成するしるし［トークン］，カード，またはその他の物の権限を電子的に剥奪し，臨時または恒久的な代替品を適切かつ厳格な管理の元に発行する損失管理手順の遵守を含む。）	○		使用時の不正な企てが検知された場合，システム管理者は登録されているユーザを不能にすることができる。 割り付けられたIDコードとパスワードを維持，発行，検査，追跡するための具体的で明確な管理を手順書に含む必要がある。 トークンもカードも使用していない。
Subpart C, §11. 300. Controls for identification codes/passwords. (Cont.) *d) "Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at the unauthorized use to the system security unit, and, as appropriate, to organizational management."*（§11. 300の続き…そのような管理とは，パスワード及び／またはIDコードの不正な使用を防止し，不正な使用におけるいかなる試みをも迅速且つ緊急に検知してシステムセキュリティ・ユニット，及び必要に応じ，組織の経営陣に報告するためのトランザクション保護を含む。）	○		3回あるいは5回（回数は設定による）ログインに失敗すると，そのユーザのアクセスは禁止される。この行為は監査証跡として記録される。ログインの成功の後に，DXAdv/AS1がファイルへの電子署名の不適切な試みを3回あるいは5回検知した場合，該当ファイルに電子署名するための以降のアクセスは全て自動的に禁止される。これ以降も，データは印字可能であり，従来の手書きの署名をすることは可能である。 DXAdv/AS1が使用時の不正な試みを検知すると，その旨画面に表示される。この表示はシステム管理者にしか消すことができない。正規のデータ収集シーケンスが中断されることは無い。 ユーザロックアウト時のEメール通知および/またはシステムリレー出力も可能。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation

DAQSTATION医薬品モデルDXAdvanced拡張セキュリティ機能の21CFR Part11対応一覧表

21 CFR Part 11要求事項 （正式規約が英文であるため，規約原文に続き括弧内に抄訳を示す）	**要求に対応？**		**コメント**
	対応	**未対応**	
Subpart C, §11. 300. Controls for identification codes/passwords. (Cont.) *e) "Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner."*（§11. 300の続き…そのような管理とは，IDコードまたはパスワード情報を記録している，あるいは生成するトークンやカード等の物が適切に機能し，不正な方法で変更が加えられていないことを確実にするためのそれらの初期および定期的検査を含む。）	非該当		トークンもカードも使用していない。

All Rights Reserved. Copyright © 2010, Yokogawa Electoric Corporation